Hastings Communications and Entertainment Law Journal

Volume 31 | Number 3 Article 2

1-1-2009

Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware

Heather Ng Osborn

Targeting Bad Behavior: Why Federal Regulators Must Treat Online Behavioral Marketing as Spyware

by
HEATHER OSBORN NG*

I. The Practice of Online-Targeted Advertising 370
A. Introduction 370
B. Background on Targeted Advertising 371
1. How It Works 371
2. Huge Growth in the Past Year and Impact of Media Consolidation 373
C. Comparing and Contrasting Spyware to Targeted Advertising 373
1. How is Spyware Similar to Targeted Advertising? 373
2. How Does Spyware Differ From Targeted Advertising? 374
II. The Threats of Unregulated Online-Targeted Advertising 375
A. Consumers Make Uninformed Choices 376
B. Power Imbalance by Ad Companies Who Use Information to Manipulate Behavior 378
C. "Distributive Justice" Concerns 380
D. Concerns About Young People's Privacy 380
E. Health Issues 381
F. Monopoly Profits by Large Companies 381
G. Misplaced and Misused Private Data 381
III. The Limitations of Current Legislation, Self-Regulation, and Proposed Legislation 382
A. Gray Area of Privacy Law and Cyberspace Law 382
B. Federal Laws 383
C. State Laws 383
D. Self-Regulation 384
E. Proposed "Do Not Track" Federal Legislation 386

---

* Mrs. Osborn Ng is a 2008 Juris Doctor graduate of University of San Francisco School of Law. She thanks Professor Susan Freiwald for her insightful comments and meticulous editing of this article. Additionally, she thanks her husband, Patrick, and daughter, Ainsley, for their love, patience and support.

IV. FTC Actions Against Spyware Activities 387
A. Spyware Problems 387
1. Lack of Meaningful Consent or No Consent 388
2. Buried Policies and Disclosures 388
3. No Notice 390
4. Difficult Removal Procedures 390
B. Why the FTC has not Pursued Targeted Advertising Companies 391
V. A New Proposed Federal Law Aimed at Online-Targeted Advertising 392
A. Introduction 392
B. Proposal 392
1. Logistics 392
2. Opt-in Program 392
3. Meaningful Notice 393
4. No Secondary Use of Information 393
5. Time Limits 393
6. Exceptions 394
C. Summary 394
VI. Conclusion 394

I. The Practice of Online-Targeted Advertising

A. Introduction

The Federal Trade Commission ("FTC") has sanctioned more than a dozen companies during the past two years for privacy violations involving the improper installation of spyware software on personal computers.[1] The spyware software allowed companies to watch and control a consumer's online activities, either without the consumer's knowledge or with the consumer's knowledge but without reasonable means for the consumer to stop it.[2] The practice of online-targeted advertising raises similar privacy issues as the use of spyware software because it also involves behind-the-scenes tracking, which most consumers never notice.[3] Online-targeted advertising allows marketing companies to engage in the same behavior as companies who use spyware—watching the consumer's Internet actions, often without the consumer's knowledge or with the consumer's knowledge but without meaningful consent or without offering the consumer the ability

1. *See infra* Part IV.

2. *See generally*, Dave Coustan, *How Spyware Works*, HOW STUFF WORKS, http://computer. howstuffworks.com/spyware.htm (last visited Mar. 19, 2009).

3. Louise Story, *F.T.C. Member Vows Tighter Controls of Online Ads*, N.Y. TIMES, Nov. 2, 2007, *available at* http://www.nytimes.com/2007/11/02/technology/02adco.html?_r=1&oref=slogin.

to stop it.[4] Nonetheless, the FTC has not brought a single action against a company that engages in improper online-targeted advertising.

The FTC's inaction highlights the need for legislative action and appropriations that spur the FTC to crack down on inappropriate online-targeted advertising. Aside from federal privacy laws that regulate financial institutions and a few state laws that require certain privacy notices to appear on websites, online-targeted advertising is largely unregulated, which permits abuse.[5]

Notably, self-regulation has failed to end advertising companies' damaging practices—such as tracking online activity without full disclosure to consumers and making opt-out procedures too difficult for the average consumer to implement.[6] In fact, efforts of a conglomerate of advertising companies who recently began an opt-out program have drawn little attention.[7] The program is difficult for consumers to utilize and the program does not apply to online-targeted advertisements that two of the largest offenders, Google and Yahoo!, deliver.[8]

This article will explain online-targeted advertising and its dangers to privacy; examine the limitations of current legislation, proposed legislation and self-regulation; review FTC cases on spyware software to demonstrate parallels to online-targeted advertising; and suggest a proposed federal law and FTC regulations specifically aimed at targeted advertising.

B. Background on Targeted Advertising

1. How It Works

Online-targeted advertising occurs when companies track the Internet activities of an individual—observing the websites visited, the time spent viewing particular webpages and the content of emails—in order to deliver personalized offers, advertisements and marketing materials.[9] Most

4. *Id.*; Dave Coustan, *How Spyware Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/spyware.htm (last visited Mar. 19, 2009).

5. *See* Letter from Jeff Chester, Executive Director, Center for Digital Democracy, and Ed Mierzwinski, Consumer Program Director, U.S. PIRG, to Deborah Platt Majoras, Chairman, Federal Trade Commission, Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices (Nov. 1, 2007), at 1-2, *available at* http://www.democraticmedia.org/files/FTCsupplemental_statement1107.pdf.

6. *See infra* Part III.D.

7. Kate Kaye, *States Could Target Behavioral Sector as Industry Battles for Self-Regulation*, CLICKZ, Nov. 4, 2007, http://www.clickz.com/show Page.html?page= 3627501.

8. *Id.*

9. *New Ways to Target Your Customer*, EMARKETER, Apr. 20, 2006, http://www.emarketer.com/Article.aspx?id=1003937.

marketing companies monitor a user's online activities secretly, although privacy policies and user agreements may alert users to the tracking.[10]

Marketers choose individualized advertisements for a user based on a variety of perceived characteristics, including the user's age, location, purchase history, contact list and web usage.[11] However, "[t]he data collected extends beyond information about consumers' views of the product to information about the consumers themselves, often including lifestyle details and even a full-scale psychological profile."[12] Targeted advertising lowers advertising costs by helping a company send its advertisements to a smaller, more selective audience that is more likely to purchase its product or utilize its services.[13]

Targeted advertising is not new, and has long been used in other media forms, such as television, postal mail, radio, and magazines.[14] But targeted advertising that takes place *online* is more privacy invasive than in older media forms because it offers marketers much more knowledge about the consumer.[15] The "*interactive* and *dynamic* tools that the Internet adds" to targeted advertisements has changed the practice.[16] For example, Google picks what "ads to show people based on the context of what they are searching for or typing about (in Gmail) at that very moment."[17] The ability of the online companies to *instantly* know *exactly* what people are doing while they are viewing the ads makes online targeting advertising more manipulative than offline targeted advertising.

Proponents of online-targeted advertising argue that it "directly subsidizes forums for more content, services, and information."[18] They also

10. *See* Louise Story, *A Push to Limit the Tracking of Web Surfers' Clicks*, N.Y. TIMES, Mar. 20, 2008, *available at* http://www.nytimes.com/2008/03/20/business/media/20adco.html?scp=1&sq=push%20limit%20tracking%20web%20surfers&st=cse. *See also infra* Part II.A.

11. *New Ways to Target Your Customer*, EMARKETER, Apr. 20, 2006, http://www.emarketer.com/Article.aspx?id=1003937.

12. DANIEL J. SOLOVE, THE DIGITAL PERSON 17 (New York University Press 2004).

13. *New Ways to Target Your Customer*, EMARKETER, Apr. 20, 2006, http://www.emarketer.com/Article.aspx?id=1003937.

14. For example, commercials for toys air during children's programming.

15. Louise Story, *F.T.C. To Review Online Ads and Privacy*, N.Y. TIMES, Nov. 1, 2007, *available at* http://www.nytimes.com/2007/11/01/technology/ 01Privacy.html?ref=technology.

16. *New Ways to Target Your Customer*, EMARKETER, Apr. 20, 2006, http://www.emarketer.com/ Article.aspx?id=1003937 (emphasis added).

17. Louise Story, *Consumer Advocates Seek a 'Do-Not-Track' List*, N.Y. TIMES, Oct. 31, 2007, *available at* http://www.nytimes.com/2007/10/31/technology/31cnd-privacy.html?_r=1& page wanted%20=print.

18. Letter from J. Trevor Hughes, Executive Director, Network Advertising Initiative, to Federal Trade Commission, Re: Network Advertising Initiative (NAI) Written Comments for the FTC's Ehavioral Advertising Town Hall Forum (Oct. 19, 2007), at 6, *available at* http://ftc.gov/os/comments/behavioraladvertising/071019nai.pdf.

argue that consumers enjoy the personalized offers, which benefit consumers by alerting them to good deals, aiding in comparison shopping, and helping them find items that they already want.[19]

2. Huge Growth in the Past Year and Impact of Media Consolidation

Online-targeted marketing is a rapidly growing industry. In 2003, advertisers spent approximately $285 million on targeted-online advertising.[20] That number jumped to $1.5 billion in 2007 and was expected to rise to $2 billion in 2008.[21]

All of the major Internet search engine companies purchased online advertising firms in 2007.[22] As a result, searching companies and advertising companies can combine data to create vast knowledge of consumers in order to deliver more accurate targeted ads. Such mergers raise questions about just how powerful targeted advertising can become. Even smaller acquisitions in the past have helped web companies piece together expansive profiles of consumers. For example, because Yahoo! and weather.com collaborated, Yahoo! can discern a user's hometown and travel plans, based on her weather searches and then deliver targeted advertising through Yahoo!'s numerous online channels.[23]

C. Comparing and Contrasting Spyware to Targeted Advertising

1. How is Spyware Similar to Targeted Advertising?

The companies that use online-targeted advertising utilize similar tactics as the ones used in spyware software. First, they use similar technology. Both types of companies watch private Internet activity using web beacons, cookies, and other invisible tracking technology to follow Internet users while they go from website to website.[24] Second, both types of companies

19. *Id.*

20. *New Ways to Target Your Customer*, EMARKETER, Apr. 20, 2006, http://www.emarketer.com/ Article.aspx?id=1003937.

21. *Id.*

22. Google purchased DoubleClick, an online ad serving and ad exchange provider; Microsoft purchased Aquantive, an ad serving firm, and AdECN, an ad exchange; AOL purchased Tacoda, a behavioral targeting firm; Yahoo! purchased RightMedia, an online ad auction network, and BlueLithium, an online advertising network. Elinor Mills, *Google Gets Even More Ambitious*, CNET NEWS, Dec. 28, 2007, http://news.cnet.com/Year-in-review-Google-gets-even-more-ambitious/ 2009-1024_3-6223832.html. *See also* Louise Story, *F.T.C. Member Vows Tighter Controls of Online Ads*, N.Y. TIMES, Nov. 2, 2007, *available at* http://www.nytimes.com/2007/11/02/ technology/02adco.html?_r=1&oref=slogin.

23. Yahoo! Media Relations, Yahoo! and Weather.Com Forge Multi-National Agreement to Provide Enhanced Weather Reports (Jan. 7, 2002), http://docs.yahoo.com/docs/pr/release908.html.

24. Dave Coustan, *How Spyware Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/spyware.htm (last visited Mar. 19, 2009); Louise Story, *A Push to Limit the*

use the information they gather in similar ways. Without a user's "informed consent," the companies base the ads on what they learn by watching. Third, both types of companies produce similar harms. They steer consumers to take a particular action, such as buy a product or visit a different website.

Finally, both spyware and targeted ads diminish autonomy, a core American value. Professor Daniel J. Solove points out the importance of consumers feeling free to *receive* information anonymously, not just share it.[25] In the context of using the Internet, Professor Julie Cohen writes: "The freedom to read anonymously is just as much a part of our tradition, and choice of reading materials just as expressive of identity, as the decision to use or withhold one's own name."[26] Allowing unregulated targeted advertising and spyware raises the risk of citizens fearing the ramifications of Internet usage—and making different choices as a result—to avoid mischaracterizations. Much of the spying and tracking occurs without actual notice, but as consumers' knowledge increases, the anonymity problem will worsen. As it stands now, targeted ads can be highly manipulative, causing consumers to lose autonomy because of the ad companies' creation of psychological profiles based on the companies' perceived notions of the user's interest, rather than the user's own choices.

2. How Does Spyware Differ From Targeted Advertising?

Although the companies that use online-targeted advertising use some of the same behind-the-scenes tactics as spyware, there are several critical differences. First, at its worst, spyware uses more invasive tactics than online-targeted advertising. In the most egregious cases, the spyware software changes settings on personal computers (such as "favorite lists" in web browsers), forces consumers to visit websites or secretly installs software that slows down a user's computer.[27] With targeted advertising, on the other hand, the consumer is less likely to know he is being watched because the only activity that takes place is the appearance of advertisements that may or may not be accurately personalized.[28] Moreover,

Tracking of Web Surfers' Clicks, N.Y. TIMES, Mar. 20, 2008, *available at* http://www.nytimes.com/2008/03/20/business/media/20adco.html?scp=1&sq=push%20limit%20tracking%20web%20surfers&st=cse.

25. SOLOVE, *supra* note 12, at 117 (Solove addresses government and private sector collection of information and the inadequate controls on privacy).

26. Julie E. Cohen, *The Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. L. Rev. 981, 1012 (1996).

27. Dave Coustan, *How Spyware Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/spyware.htm (last visited Mar. 19, 2009).

28. As consumers become increasingly aware of online tracking, the anonymity problem will deepen because consumers will realize that all companies are tracking them.

in targeted advertising, the user must take the affirmative step to click on a targeted advertisement. In contrast, in spyware, the computer programming forces the user to view certain information, without active user participation.

Both technologies cause different harms. The most egregious harms caused by spyware involve tangible harms such as taking physical control of a user's computer. The harms of targeted ads are not as physically invasive, so in that sense the harms are more subtle.[29]

Finally, one of the biggest differences between spyware and online-targeted advertising is the ability of the user to more easily remove spyware, compared to the difficultly of stopping targeted advertising. First, numerous companies offer free anti-spyware programs.[30] This protection is not foolproof, but at least it provides some help in stark contrast to the lack of such programs to prevent targeted advertising. Secondly, it is easier to stop spyware than to stop targeted advertising because users can change the browser settings on their computers to block spyware, but such options are usually not available for online tracking.[31]

II. The Threats of Unregulated Online-Targeted Advertising

The privacy harms of unregulated online-targeted advertising are not entirely clear due to the novelty of the practice. In comparison, spyware presents much more tangible and obvious harms because the practice involves the *physical* taking over of personal computers.

Professor Daniel J. Solove explains that much of the harm caused by unregulated actions that erode privacy, such as online-targeted advertising, are a "slow series of relatively minor acts which gradually begin to add up."[32] Solove compares the harms of unregulated privacy problems to environmental harms, which numerous actors cause, each doing a series of small acts that cause serious damage as a whole.[33] The numerous harms that unregulated targeted ads cause include consumers making uninformed choices about how much information to share, corporations manipulating behavior, and marketers deepening the economic divide by treating

29. *See* discussion *infra* Part I.B.1.

30. Such companies include Spybot (http://www.safer-networking.org/en/index.html) and Ad-Aware (http://www.lavasoftusa.com/).

31. According to an article written for consumers, one method of stopping Spyware is to disable Active-X on the browser if you are using the current Microsoft Windows operating system. However, doing so can "disallow the legitimate uses for Active-X, which may interfere with the functionality of some Web sites." Dave Coustan, *How Spyware Works*, HOW STUFF WORKS, http://computer. howstuffworks.com/spyware.htm (last visited Mar. 19, 2009).

32. Daniel J. Solove, *"I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 769 (2007).

33. *Id.*

individuals differently based on socioeconomics. This paper discusses these harms in detail below.

A. Consumers Make Uninformed Choices

Privacy experts warn that consumers make uninformed choices about how much personal information to share, and whether to opt out of targeted advertising.[34] For example, they point out that most consumers accept default privacy settings—on both web browsers and web sites—which highlights the need for regulation.[35] In accepting default privacy terms, the consumers consent to tracking for online-targeted advertising, but the question is whether such *passive* consent should be deemed *meaningful* consent.

Privacy experts warn that small bits of seemingly innocuous information can slowly come together to paint a more detailed picture about a user's online activity than the user ever intended to share.[36] Perhaps consumers are accepting default privacy policies because they lack knowledge about the risks of sharing too much personal information online.[37]

Likewise, before federal regulators took action, consumers were making uninformed choices about spyware. Consumers were being tricked into downloading spyware just as consumers are being tricked into accepting online-targeted ads. Companies buried important disclosures in hard-to-read user agreements and consumers were largely ignorant of the extent to which the companies were using their personal information.

Marketing companies in favor of online tracking argue that the nature of the Internet has led to "more consumer privacy safeguards . . . than any other marketing channel."[38] Still, there is inadequate protection. Although

34. *See infra* notes 35-36 and accompanying text.

35. Paul M. Schwartz, *Property, Privacy and Personal Data,* 117 HARV. L. REV. 2055, 2081 (2004) ("Behavioral economics scholarship has demonstrated that consumers' general inertia toward default terms is a strong and pervasive limitation on free choice.").

36. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373, 1398-99 (May 2000). Cohen argues that data processors do not want to share exactly how personal information is being used because some of the uses are so offensive that most consumers would likely object. For example, personal information can be used for "employment decisions and classifications by health insurance providers that exclude or disadvantage genetic or medical 'have-nots,' employment or housing decisions based on perceived personality risks; and employment or housing decisions based on sexual or religious preferences." *Id.* at 1399.

37. *Id.* at 1432.

38. Letter from J. Trevor Hughes, Executive Director, Network Advertising Initiative, to Federal Trade Commission, Re: Network Advertising Initiative (NAI) Written Comments for the FTC's Ehavioral Advertising Town Hall Forum (Oct. 19, 2007), at 10, *available at* http://ftc.gov/os/ comments/behavioraladvertising/071019nai.pdf.

consumers can stop some of the tracking by utilizing various anti-tracking programs, such programs are not highly effective.[39]

Companies can disclose privacy policies in greater detail online than offline, making it easier to inform consumers about the use of personal information and help them make informed choices. Marketers point out this is one reason that privacy proponents are too worried about online tracking.[40] Even so, consumers face difficulty discovering the full extent of the tracking to which they are being subjected, even with the privacy policies available on virtually every website.[41]

The sheer multitude of privacy policies governing consumers' Internet activities makes it hard to stay informed; search engines, news outlets, online stores, email services, and music download sites each have their own privacy policies. Even when notice is available, consumers face increasing difficulty understanding the numerous polices that apply. Consumers who read *USA Today* online, for example, will be subject to *USA Today's* online privacy policy, which includes a list of over two dozen third-party companies that may track the consumer in various ways when a user clicks on an advertisement from the *USA Today* website.[42] However, once the user goes to the third-party websites, different privacy policies apply.

Current privacy policies of some of the largest websites that track online activity to create targeted ads include loopholes that permit abuse and lead consumers to misunderstand the policies. The PayPal privacy policy, for example, has a catch-all clause stating that additional information may be collected "from or about you in other ways not specifically described here."[43] DoubleClick, one of the largest online advertising firms that engage in online-targeted advertising, states that it can change its privacy policy at any time.[44]

The average consumer may not be able to understand all of the privacy implications set forth in a privacy policy due to the way companies phrase information to make it seem more palatable. For example, the online store

39. *See* discussion, *infra* Part III.D.

40. Letter from J. Trevor Hughes, Executive Director, Network Advertising Initiative, to Federal Trade Commission, Re: Network Advertising Initiative (NAI) Written Comments for the FTC's Behavioral Advertising Town Hall Forum (Oct. 19, 2007), at 10, *available at* http://ftc.gov/os/ comments/behavioraladvertising/071019nai.pdf.

41. Cohen, *supra* note 36, at 1397 (noting that consumers face "enormous difficulty" determining how personal information is being used).

42. USATODAY.com, Third-Party Advertisers and Ad Servers (Dec. 18, 2007), http://www.usatoday.com/marketing/advertiser-list.htm.

43. PayPal.com, Privacy Policy for PayPal Services (including PayPal Money Market Fund), https://www.paypal.com/privacy (last visited Mar. 3, 2008).

44. DoubleClick.com, Privacy Policy for Information Use at this Website (Aug. 14. 2008), http://www.doubleclick.com/privacy/.

for Apple computers writes appealing language in its policy on third-party information sharing: "There are also times when it may be advantageous for Apple to make certain personal information about you available to companies that Apple has a strategic relationship with . . . ."[45]

Finally, consumers are not in a position to bargain for more privacy because online-targeted advertising usually arises under boilerplate user contracts. If a person does not consent to Google's policy of online tracking, she has little recourse except to use an inferior search engine. As Professor Julie Cohen points out, the problem is the fact that *vendors* decide what the choices about the usage of personal information will be, not the consumers.[46] Consumers may decide to freely share private information because they assume, correctly so, that the transaction is non-negotiable.[47]

B. Power Imbalance by Ad Companies Who Use Information to Manipulate Behavior

The growing power imbalance between companies and consumers stems from the sheer volume of information that companies collect for marketing purposes. Consider an introduction to a report for potential marketers about online-targeted advertising: "Users reveal their interests by the keywords they enter—that's the secret behind search advertising's great success. For the first time, marketers have some idea of 'what's going on' in the mind of the consumer *at the moment of contact* (emphasis added)."[48] Such intimate knowledge of the consumer is just what privacy experts fear. Professor Paul Schwartz predicts that if personal information can be freely shared, people will "decline to engage in a range of different social interactions due to concerns about use of personal information."[49]

Furthermore, privacy advocates, including the Center for Digital Democracy and U.S. Public Interest Research Group, argue that characterizing consumers with "often-flippant taxonomy"—such as Shopaholics, Penny Pinchers, Lonely Hearts, and Hardcore Gamers—"masks the crass, manipulative nature of such digital stereotyping."[50]

45. Apple.com, Apple Customer Privacy Policy, http://www.apple.com/legal/privacy/ (last visited Mar. 8, 2008).

46. Cohen, *supra* note 36, at 1397.

47. *Id.*

48. *Online Ad Targeting: Engaging The Audience*, EMARKETER, Apr. 2006, http://www.emarketer.com/Report.aspx?code=targeting_may06&src=report_summary_reportsell.

49. Schwartz, *supra* note 35, at 2089.

50. Letter from Jeff Chester, Executive Director, Center for Digital Democracy, and Ed Mierzwinski, Consumer Program Director, U.S. PIRG, to Deborah Platt Majoras, Chairman, Federal Trade Commission, Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices (Nov.

Marketers in favor of online-targeted advertising argue that allowing more profiling will lead to better products offered and will provide consumers with information they already want.[51] However, Professor Julie Cohen counters that such practices constitute manipulation because advertising does not simply reflect "pre-existing desires."[52] Even benign discrimination categorizes people as they may not wish.[53] "The view of human nature reinforced by data-processing algorithms," Cohen asserts, "is both unforgiving and ungenerous."[54] Moreover, it leaves little room for "second chances."[55]

Marketing companies also provide overly tempting offers based on intimate knowledge of their consumers. For example, sub-prime mortgage loan practices demonstrate a marketer's ability to piece together customer information, such as her domicile, homeownership status, and income level, in order to send offers to purchase homes that could be beyond her means.[56] While such targeting takes place off the Internet, it can be much more manipulative when it happens online because of the marketer's precise knowledge about the consumer based on a psychological profile and current online activities, which enables the marketer to formulate a carefully-crafted ad that increases susceptibility to the offer.[57]

The power imbalance raises concerns about diminishment of autonomy. If online Internet tracking continues without regulation, some privacy experts predict that the experience of being constantly watched will "constrain, ex ante, the acceptable spectrum of belief and behavior" and will incline people's choices toward the "bland and the mainstream."[58] Personal autonomy requires "a zone of relative insulation from outside scrutiny and interference . . . ."[59] Regulating targeted advertisers will help to ensure that using the Internet does not subject consumers to constant outside inspection.

1, 2007), at 3, *available at* http://www.democraticmedia.org/files/FTCsupplemental_statement 1107.pdf.

51. Letter from J. Trevor Hughes, Executive Director, Network Advertising Initiative, to Federal Trade Commission, Re: Network Advertising Initiative (NAI) Written Comments for the FTC's Behavioral Advertising Town Hall Forum (Oct. 19, 2007), at 6, *available at* http://ftc.gov/os/ comments/behavioraladvertising/071019nai.pdf.

52. Cohen, *supra* note 36, at 1407.

53. *Id.*

54. *Id.* at 1408.

55. *Id.*

56. This example is a hypothetical scenario that demonstrates potential dangers of online-targeted advertising.

57. *See* discussion *supra* Part I.B.2.

58. Cohen, *supra* note 36, at 1426.

59. *Id.* at 1424.

C. "Distributive Justice" Concerns

Targeted-online marketing presents the problem of "distributive justice." Those in higher and lower income brackets experience harm in different ways, but both groups suffer.

People in higher income brackets suffer because their data generates the most useful data for marketers, meaning the data processors will more aggressively seek their information, and users will have to go to greater lengths to protect their privacy online. On the other hand, people in lower income brackets are not included when marketing companies offer those in the higher income brackets special deals on a variety of items—from medicine to clothing to food. For example, people who are deemed to have more money may receive online advertising for breakthrough drugs and treatments for serious medical conditions, while those with less money to pay for such services will not receive the ads.

Cohen points out the harms in rigid categorization of people.[60] Although Cohen admits that the categorization will sometimes be fair, she says a society that relies on such categories "as a means of allocating economic opportunity" should be the subject of debate in the U.S. in order to determine if the government should limit the sharing of personal information.[61]

D. Concerns About Young People's Privacy

The Children's Online Privacy Protection Act of 1998 ("COPPA") prohibits the online collection and use of personal information for children ages thirteen and younger.[62] However, some commentators question if regulators enforce the law aggressively enough with regards to online-targeted ads,[63] and have asked for COPPA explicitly to ban targeted advertising for children.[64] One possible consequence of allowing targeted ads for children is increasing the childhood obesity epidemic because of tempting targeted ads for junk food sent to children online.

Another drawback of the law is that children over age thirteen receive no protection, and the teen-age bracket is one of the most vulnerable because teens are less likely than adults to understand the long-term

60. *Id.* at 1408.

61. *Id.*

62. 15 U.S.C. §§ 6501–6506.

63. Letter from Jeffrey Chester, Center for Digital Democracy, and Ed Mierswinski, USPIRG, to Deborah Platt Majoras, Chairman, Federal Trade Commission, Calling for Action on Behavioral Targeting (Nov. 12, 2007), *available at* http://www.democraticmedia.org/news_room/letters/Letter_re_Behavioral_Targeting.

64. Stefanie Olsen, *Group Calls for Teen Privacy Protections on Facebook, MySpace*, CNET NEWS, Apr. 10, 2008, http://news.cnet.com/8301-10784_3-9915769-7.html?tag=nefd.top.

consequences of sharing personal information online for tracking.[65] Teens are also more susceptible to targeted advertisements that are tailored to their psychological weaknesses.[66]

E. Health Issues

Concerns about online-targeted advertising are especially heightened when it comes to pharmaceutical ads. Advertisements about highly sensitive health problems that are delivered to Internet users after marketers determine the users have a particular illness based on their Internet activity are especially egregious. Drug companies who use online-targeted advertising may have enough intimate information about a consumer to be able to give tempting offers for drugs that may not be in the consumer's best interest. Recently, several industry members voluntarily decided to restrict usage of targeted advertising because of such concerns.[67] Most industrialized countries other than the U.S. prohibit targeted consumer ads for drugs.[68]

F. Monopoly Profits by Large Companies

Large corporations can spend more money on online-targeted advertising than smaller companies, which raises the risk of monopolization. Although marketing analysts stress that targeted advertisements deliver more sales for a lower cost, the price for such advertising remains high when compared to traditional Internet advertisements[69] so large companies can more easily afford the advertisements.

G. Misplaced and Misused Private Data

The massive amount of data collected for online-targeted advertising may be misplaced and misused. Few systems exist to ensure the data stays out of the wrong hands. "In other words, the problem is not simply a lack of individual control over information, but a situation where *nobody* is exercising meaningful control over the information."[70] Executives of

65. *Id.*

66. *Id.*

67. Peter Loftus, *Drug Companies Trim Advertising Spending, Tweak Approach*, DOW JONES NEWSWIRES, Dec. 9, 2008, *available at* http://english.capital.gr/NewsPrint.asp?id=635012.

68. *Direct-to-consumer advertising in the United States*, SOURCEWATCH, http://www.sourcewatch.org/index.php?title=Direct-to-consumer_advertising_in_the_United_States (last visited Apr. 4, 2009).

69. *See* Scott Buresh, *The Evolution of Online Advertising Technology – More Targeting, Less Privacy (Part One)*, MEDIUM BLUE, http://www.mediumblue.com/newsletters/advertising-technology.html (last visited Apr. 4, 2009).

70. SOLOVE, *supra* note 12, at 53.

corporations will often wait for external forces to act, i.e., government regulators, before improving data collection practices.[71]

Moreover, companies may use information for a different purpose than that which consumers intended, especially when companies sell the information for secondary uses without consumer consent. Finally, third parties may gain unauthorized access to stored information because companies do not operate under standardized procedures for keeping the information secure.

III. The Limitations of Current Legislation, Self-Regulation, and Proposed Legislation

A. Gray Area of Privacy Law and Cyberspace Law

Online-targeted advertising is not explicitly regulated, and no federal or state cases speak to the matter yet, which means that consumers enjoy little legal protection against damaging practices. Attempts at self-regulation, while laudable, are deeply flawed. As such, the practice of online-targeted advertising represents a gray area of the law.

Under federal law, deceptive trade practices of any kind violate the Federal Trade Commission Act.[72] Additionally, the Electronic Communications Privacy Act makes it unlawful for companies to gain unauthorized access to customers' stored e-mails while they are in transit to the recipient.[73] Portions of such laws could be used to regulate online-targeted advertising, but do not directly address it.

In contrast, federal laws and a few state laws specifically regulate spyware. The Computer Fraud and Abuse Act banned unauthorized installation of spyware at the federal level.[74] The state of Utah banned spyware in the Spyware Control Act[75] and California banned spyware in the Consumer Protection Against Computer Spyware Act.[76]

The following section will discuss federal laws, state laws, and proposed self-regulation efforts that relate to online-targeted advertising and explain the benefits and pitfalls of each.

71. *Id.* (quoting H. JEFF SMITH, MANAGING PRIVACY: INFORMATION TECHNOLOGY AND CORPORATE AMERICA 162 (University of North Carolina Press 1994)).

72. 15 U.S.C.S. § 45(a)(2) (LexisNexis 2008).

73. 18 U.S.C. § 2701 (LexisNexis 2008).

74. 18 U.S.C.S. § 1030 (LexisNexis 2008).

75. UTAH CODE ANN. §§ 13-40-101 - 13-40-302 (2008).

76. CAL. BUS. & PROF. CODE § 22947.2 (Deering 2008).

B. Federal Laws

No federal laws specifically cover online-targeted advertising, but at least two laws restrict financial institutions' use of personal information. Under the Gramm-Leach-Bliley Act, financial institutions must give customers privacy notices that explain collection and sharing practices, and companies must allow customers to limit information sharing.[77] The drawback to this law is that it only applies to financial institutions, and targeted advertising takes place in many other sectors of the economy.[78]

Under the Fair Credit Reporting Act, the federal government established fair practices for the use of personal information relating to a consumer's credit report.[79] This includes rights of data quality, the right to access and correct data, security of data, use limitations on data, and requirements for destroying data.[80] The law addresses many of the areas of concern raised by online-targeted advertising, including data security, but it does not apply to most online-targeted advertising because it covers only credit reports. The law, however, provides a valuable framework for how the federal government should limit the use of personal information to the purpose for which it is collected.

C. State Laws

California and New York both have very strong consumer privacy protection laws in place. In California, the Online Privacy Protection Act of 2003 requires online services collecting personal information about California residents through a commercial web site to conspicuously post a privacy policy and comply with it.[81] The law requires only disclosure; it does not regulate the content of privacy policies or require companies to draft precise, understandable policies. A prime result is PayPal's privacy policy, discussed above, which states that PayPal "may collect additional information from or about you in other ways not specifically described here."[82] The company posts this policy in a conspicuous place, thus it complies with the law. But PayPal's policy illustrates that the law merely

77. 15 U.S.C.S. §§ 6801–6809 (LexisNexis 2008).

78. 15 U.S.C.S. § 6805 (LexisNexis 2008).

79. 15 U.S.C.S. § 1681 (LexisNexis 2008).

80. 15 U.S.C.S. § 1681s-2 (requiring furnishers of information to consumer reporting agencies to provide accurate information and to notify consumers when negative information is shared with a third party); 15 U.S.C.S. § 1681i (explaining procedures in case of disputed accuracy); 15 U.S.C.S. § 1681w (requiring proper disposal of information); 15 U.S.C.S. § 1681b (requiring limited use of information collected).

81. CAL. BUS. AND PROF. CODE §§ 22575-22579 (Deering 2008).

82. PayPal.com, Privacy Policy for PayPal Services (including PayPal Money Market Fund), https://www.paypal.com/privacy (last visited Mar. 3, 2008).

requires disclosure about the myriad ways companies can use and share personal information, but does not demand privacy protection.

New York's Internet Security Privacy Act and its Model Policy provide strong online privacy protection, but they apply only to state agencies.[83] The Model Policy provides robust privacy protections for users of government websites, but private websites need not comply.[84] Under the Model Policy, government agencies must provide users with specific information about data collection and use.[85] Moreover, the language is clearer than in typical privacy policies, thus easier to understand.[86] Finally, the Model Policy requires that sites explain the particular technology that is tracking Internet activity.[87]

In conclusion, California's privacy law is too vague to provide substantial protection because it only requires *disclosure* of policies—which may be flawed—and permits companies to engage in extensive privacy-eroding tracking practices. New York's privacy law, on the other hand, provides a Model Policy that provides extensive consumer protection, but its application is limited to government agencies' websites.

D. Self-Regulation

Three main self-regulation efforts include the Network Advertising Initiative ("NAI") (a consortium that administers an opt-out program), P3P (an organization that plans to set international standards for opt-out and disclosure procedures) and TRUSTe (a private auditing service).[88] The failure of these three initiatives demonstrates the need for federal legislation.

The NAI, a consortium of online advertising companies, allows consumers to opt-out of targeted advertising that come from NAI members.[89] Consumers may complete a form on the NAI website indicating which advertising companies may not track them.[90] Consumers must access this form from the web browser on his or her personal computer. Under this

83. N.Y. Tech. Law §§ 201- 208 (McKinney's 2008).

84. JAMES T. DILLON, NEW YORK STATE BEST PRACTICE GUIDELINE, GUIDELINES FOR INTERNET PRIVACY POLICIES, Part 1 (2002), http://www.oft.state.ny.us/policy/NYSGuidelineG02-001.htm.

85. *Id.* at Part 2.

86. At least one study has found that "people with a high school education can easily understand only 1 percent of the privacy policies of large companies." Louise Story, *F.T.C. Member Vows Tighter Controls of Online Ads*, N.Y. TIMES, Nov. 2, 2007, *available at* http://www.nytimes.com/2007/11/02/ technology/02adco.html?_r=1&oref=slogin.

87. *Id.* at Part 4.6.

88. *See infra* notes 89, 94-95.

89. Network Advertising Initiative, http://networkadvertising.org (last visited Mar. 3, 2008).

90. Network Advertising Initiative, Opt Out of Behavorial Advertising, http://networkadvertising.org/managing/opt_out.asp (last visited April 4, 2009).

program, small businesses can continue to use targeted advertising "affordably, efficiently, and effectively" so long as they comply with consumers' opt-out choices.[91] The problem with the NAI is that a user must revisit the NAI website to update her opt-out choices if she purchases a new computer, uses a different computer, deletes opt-out cookies, or changes settings on her computer.[92] Finally, although NAI's membership is growing, not all targeted advertisers have joined the consortium, limiting its effectiveness.[93]

Another effort at self-regulation is the Platform for Privacy Preferences, known as P3P, which would enable websites to disclose their practices in "a standard format that can be retrieved automatically and interpreted easily by user agents."[94] Under this framework, the user would choose which websites could track her based on each website's privacy policy, which the web browser would check against the privacy preferences that the user had preset in her web browser. The user would have to approve any transaction that contradicted her preset privacy preferences. If implemented well, this program would allow consumers to make highly individualized, transaction-by-transaction choices about sharing private information, rather than a take-it-or-leave-it approach to entire websites. P3P backers have been trying to launch the program since the 1990s, but have run into logistical roadblocks. If implemented, P3P may be difficult for the average consumer to implement because it would require consumers to spend time managing their privacy preferences. Also, websites are not obliged to participate, meaning the websites would not have to allow the preset privacy preferences to be followed.

The final self-regulation effort is the use of a private company, TRUSTe, to provide "seals of approval" on websites that indicate the level of privacy protection being offered.[95] TRUSTe acts as an auditor, reviewing the company's privacy policies to ensure each company is following the

91. Letter from J. Trevor Hughes, Executive Director, Network Advertising Initiative, to Federal Trade Commission, Re: Network Advertising Initiative (NAI) Written Comments for the FTC's Ehavioral Advertising Town Hall Forum (Oct. 19, 2007), at 7, *available at* http://ftc.gov/os/comments/behavioraladvertising/071019nai.pdf.

92. Network Advertising Initiative, FAQs, http://networkadvertising.org/managing/faqs.asp (last visited April, 4, 2009).

93. The two largest companies using targeted advertising, Google and Microsoft, are not currently NAI members, but recently submitted applications. Kate Kaye, *States Could Target Behavioral Sector as Industry Battles for Self-Regulation*, CLICKZ, Nov. 4, 2007, http://www.clickz.com/show Page.html?page= 3627501.

94. Platform for Privacy Preferences (P3P) Project, What is P3P?, http://www.w3.org/P3P/ (last visited Mar. 8, 2008).

95. TRUSTe.com, Who's On the List, http://www.truste.org/about/member_list.php (last visited Apr. 14, 2008) (listing hundreds of TRUSTe's customers, including most of the household-name websites, such as eBay, Microsoft, and Yahoo!).

privacy standards to which it agreed.[96] It also provides a dispute resolution service for consumers.[97] A major advantage of the program is its widespread adoption, which shows that both companies and consumers give it some degree of credence.[98] Several of the largest websites use TRUSTe, including eBay, Microsoft, AOL and Yahoo!.[99] However, the program provides few consequences for breaches of privacy policies, and consumers may not notice if the TRUSTe seal of approval is temporarily removed from the website due to a breach.[100] Moreover, like California's online privacy law, the TRUSTe self-auditing system requires compliance only with the privacy policies that each company establishes for itself.

E. Proposed "Do Not Track" Federal Legislation

Various privacy experts have proposed a "do not track" registry akin to the current "do not call registry."[101] However, this could cause more privacy problems than it fixes. The proposal, suggested by the Center for Digital Democracy and 10 advocacy groups, calls for a national database of consumers who have requested removal from online tracking.[102] The web browsers would be responsible for blocking or deleting "persistent unique identifiers" such as cookies in order to block ad companies' access to consumers who had opted out.[103]

The "do not track" plan would be expensive and technically challenging to implement. Because of jurisdictional issues, internationally run websites would largely be exempt. Privacy experts fear that a "do not track" program would allow the government to collect too much personally identifiable information from the public, which would cause a high risk of government misuse of the data due to unreliable "institutional structures and

96. TRUSTe.org, Privacy is Everyone's Business, http://www.truste.org/about/our_services.php (last visited April 4, 2009).

97. *Id.*

98. TRUSTe.org, Who's On the List, http://www.truste.org/about/member_list.php (last visited Apr. 14, 2008).

99. *Id.*

100. TRUSTe.org, General TRUSTe Application: Frequently Asked Questions, http://www.truste.org/businesses/faq_general.php (last visited April 4, 2009).

101. Letter from Ari Schwartz, Deputy Director, Center for Democracy and Technology, et al., to Donald S. Clark, Secretary, Federal Trade Commission, In advance of the FTC Town Hall, "Ehaviroal Advertising: Tracking, Targeting, and Technology," to be held November 1-2, 2007 in Washington, D.C. (Oct. 31, 2007), *available at* http://www.cdt.org/privacy/20071031consumerprotectionsbehavioral.pdf.

102. The CDT's proposal, only a few months old, provides only a rough outline for the registry. *Operation of the Do Not Track List*, CENTER FOR DEMOCRACY AND TECHNOLOGY, http://www.cdt.org/privacy/ 20071031donottrack.pdf (last visited Apr. 14, 2008).

103. *Id.*

architectures of power."[104] For the first time, the government would have an extensive database of citizens' computer IP addresses. Furthermore, the proposal's call for an opt-out system, rather than an opt-in system, may lead to consumers to avoid signing up due to inertia. Consumers may have false hopes of the program protecting them against online tracking if they enter the registry, despite the possibility that the registry would not protect all private information.

The registry's biggest benefit is giving consumers what they want. Studies show that most consumers like targeted ads,[105] and this program would let consumers choose to receive targeted advertisements if they like. Nonetheless, the do-not-track proposal is not the best way to protect consumers from online-targeted advertising because of its expense and the risk that the government will use the extensive consumer data it collects—including the IP addresses of citizens—to further track individuals for its own purposes, such as surveillance.

IV. FTC Actions Against Spyware Activities

A. Spyware Problems

From 2005 to 2007, the FTC filed numerous complaints and settled with various companies for improper use of spyware to track and control online activity.[106] However, the FTC has not taken a single action to prohibit online-targeted advertising, despite numerous complaints by public advocacy groups.[107]

The FTC's aggressive campaign against spyware illustrates that spyware raises many of same legal issues—and consumer-harming behavior—that are apparent in online-targeted advertising: inadequate consent, buried disclosures, and difficult removal procedures. As such, the

104. SOLOVE, *supra* note 12, at 186-87 (noting "lack of control over government information gathering" in the past 50 years).

105. Matthew G. Nelson, *Users Request More Targeted Ads, Study Says*, CLICKZ, Oct. 12, 2007, http://www.clickz.com/showPage.html?page=3627288 ("While the majority of U.S. Web users say they see too many ads, they wouldn't mind having those ads better targeted to their needs.").

106. *See infra* notes 108, 113, and 115 and accompanying text.

107. Letter from Jeff Chester, Executive Director, Center for Digital Democracy, and Ed Mierzwinski, Consumer Program Director, U.S. PIRG, to Deborah Platt Majoras, Chairman, Federal Trade Commission, Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices (Nov. 1, 2007), at 1, *available at* http://www.democraticmedia.org/files/FTCsupplemental_statement1107.pdf (noting how nothing has changed since the the Center for Digital Democracy (CDD) and the US Public Interest Research Group (USPIRG) filed a complaint with the FTC against Microsoft and other companies for unfair and deceptive online-targeted marketing practices in November 2006).

FTC actions on spyware suggest that the FTC should also take action against companies engaging in improper online-targeted advertising.

1. Lack of Meaningful Consent or No Consent

Several FTC spyware cases questioned whether consumers had consented to installing spyware and, specifically, whether consumers had provided meaningful consent.

In a complaint filed against Sony BMG Music Entertainment in 2007, the FTC stated that Sony failed to adequately disclose its tracking practices.[108] When the user connected to the Internet, the media player that Sony sold as a bundle with its CDs automatically connected to Sony, showing Sony the album being played, which Sony used to generate promotional materials for the user.[109] However, Sony did not provide notice of this practice on the jewel case holding the CD.[110] Furthermore, after purchasing the CD, Sony required the user to accept the user agreement, or the computer would eject the CD.[111] Finally, even if the consumer rejected the agreement, some of the tracking software remained on the computer.[112]

Sony's practices raised problems that online-targeted advertising presents today. Users have little control over how a company uses personal information because of one-sided, boilerplate user agreements that must be accepted in order to access a website. Moreover, user contracts do not always make it clear that agreeing to the contract means the consumer has consented to extensive tracking. Finally, in some cases, companies collect information before a user has a chance to reject a user agreement that outlines the usage of personal information.

2. Buried Policies and Disclosures

In the FTC case *In the Matter of Advertising.com,* the FTC stipulated that spyware that watched or controlled Internet activities without the consumers' prior knowledge because policies on such activities were *buried* in the End User License Agreements ("EULAs") constituted deceptive practices.[113] In the case, the FTC noted disfavorably that the disclosure stating that information could be shared with third parties in exchange for

108. Complaint at 4, In the Matter of Sony BMG Music Entertainment, FTC File No. 062-3019 (June 28, 2007), *available at* http://www.ftc.gov/os/caselist/0623019/0623019cmp070629.pdf.

109. *Id.* at 2.

110. *Id.*

111. *Id.*

112. *Id.*

113. Complaint at 2-3, In the Matter of Advertising.com, FTC File No. 042-3196 (Sept. 12, 2005), *available at* www.ftc.gov/os/caselist/0423196/050803comp0423196.pdf.

the consumers' use of the software was in small print and located under several other hyperlinks, which made it hard to find.[114]

In another case, the FTC took issue with a spyware program that Odysseus Marketing installed on personal computers without providing conspicuous disclosures.[115] When users downloaded the software, the only notice that Odysseus could share a user's personal information with third parties appeared in the middle of a two-page EULA.[116] Moreover, Odysseus did not require users to read the EULA in order to accept it (they only had to check a box stating they had accepted it) and Odysseus did not adequately disclose the consequences of signing the EULA through the labeling of the hyperlink to the EULA.[117]

The FTC does not tolerate buried disclosures regarding companies' policies on tracking Internet activity and sharing information with third parties.[118] In similar fashion, companies bury their disclosures about online-targeted advertising. For example, Yahoo! shares its privacy policy in detail, and provides links to the specific privacy policies that apply to the dozens of services that Yahoo! operates.[119] Nonetheless, in the midst of all of the details, it includes buried disclosures. For example, halfway through one of the numerous privacy policies, Yahoo! notes:

> Yahoo! "targets" some ads to users that may fit a certain profile—for example, men interested in financial services. Yahoo! does not provide any personal information to the advertiser when you interact with or view a targeted advertisement. However, when you view or interact with an ad *the possibility exists that the advertiser will make the assumption that you meet the targeting criteria* used to display the ad.[120]

114. *Id.* at 2.

115. Complaint for Injunction and Other Equitable Relief at 3, FTC v. Odysseus Marketing, No. 1:05-cv-00330-SM (D. N.H. Sept. 21, 2005), *available at* www.ftc.gov/os/caselist/0423205/050929comp0423205.pdf.

116. *Id.* at 6.

117. *Id.*

118. *Id.* at 11 (noting that "failure to disclose these facts, in light of the representation made, constitutes a deceptive act or practice . . . ."); Complaint at 5, In the Matter of Advertising.com, FTC File No. 042-3196 (Sept. 12, 2005), *available at* www.ftc.gov/os/caselist/0423196 /050803comp0423196.pdf.

119. Yahoo! Privacy, What This Privacy Policy Covers, http://info.yahoo.com/privacy/us /yahoo (last visited April 4, 2009).

120. Yahoo! Privacy, Third Party and Affiliate Cookies on Yahoo!, http://info.yahoo.com/privacy/us/yahoo/thirdparties/details.html (last visited Apr. 4, 2009) (emphasis added).

This example shows that disclosures, even lengthy ones, can fail to specify the company's actual use of private information. Yahoo!'s policy also notes that it frequently acquires other companies, but that users must refer to the policies of the acquired companies.[121] This web of information, with disclosures buried within disclosures, highlights the same issue that the FTC addressed in the Advertising.com and Odysseus Marketing complaints, and shows the need for the FTC to take action against online-targeted advertising.

3. No Notice

In one of the most egregious FTC cases that addressed spyware, *FTC v. Odysseus Marketing*, consumers had no notice—constructive or actual—about a subset of the spyware software that Odysseus installed on their personal computers.[122] Lack of notice is unlikely to be a problem today because virtually all companies provide privacy notices.

4. Difficult Removal Procedures

The FTC has taken issue with difficult removal procedures for spyware once installed. The U.S. District Court for the Central District ordered Digital Enterprises to include an "uninstall" program for all individuals who had agreed to have spyware programs on their computers and to ensure the uninstall program was easy to locate on the user's computer.[123] The court also ordered the company to provide *complete* terms of use, rather than partial terms, before the end of the download of the spyware program.[124]

In the *Sony* case, the FTC took issue with the software programs because it took more than reasonable efforts to uninstall the spyware programs.[125] In addition, the FTC chastised both Digital Enterprises and DirectRevenue for adding provisions that overrode a consumer's decision to uninstall a spyware program.[126]

---

121. Yahoo! Privacy, Yahoo! Acquired Companies, http://info.yahoo.com/privacy/us/yahoo/acquiredcompanies (last visited Mar. 29, 2009).

122. FTC v. Odysseus Marketing, 2006 U.S. Dist. LEXIS 30230, at *11-12 (D. N.H. Apr. 19, 2006).

123. Settlement Agreement and Stipulated Final Order For Permanent Injunction and Monetary Relief at 10, FTC v. Digital Enterprises, Inc., No. CV06-4923 CAS (AJWx) (C.D. Cal. Sept. 5, 2007), *available at* http://www.ftc.gov/os/caselist/0623008/070905digitalenterprisesstipfnl.pdf.

124. *Id.* at 7.

125. In the Matter of Sony BMG Music, at 4.

126. Complaint for Permanent Injunction and Other Equitable Relief at 17-18, FTC v. Digital Enterprises, Inc., et al., No. CV06-4923 CAS (AJWx) (C.D. Cal. Aug. 8, 2006), *available at* http://www.ftc.gov/os/caselist/0623008/060808movielandcmplt.pdf; Complaint at 6, In the Matter of DirectRevenue LLC, FTC File No. 052-3131, (June 26, 2007), *available at* http://ftc.gov/os/caselist/0523131/0523131cmp070629.pdf.

Difficult removal procedures also occur in online-targeted advertising. Stopping online-targeted advertising poses challenges because such programs as the NAI and TRUSTe cover only a portion of the companies involved. For example, Yahoo! tells users that to stop tracking by third-party advertising companies whose ads appear on Yahoo!, the users must individually contact the third-party advertising companies.[127] Yahoo! lists more than 50 advertising companies to contact.[128] As in the *Sony* case, it would require more than reasonable care for the average consumer to manage the time-consuming process of doing so.

B. Why the FTC has not Pursued Targeted Advertising Companies

The FTC has never taken action against a company for online-targeted advertising even though the practice raises many of the same legal issues and harms as spyware use. There are several possible reasons for this. First, online-targeted advertising is newer than spyware and has not garnered as much public attention. The FTC has limited financial resources for cracking down on consumer-harming behaviors, and it will most often choose to pursue practices that are more notorious. Second, while many of the harms that targeted advertising causes are similar to spyware, the harms in targeted advertising tend to be subtler.[129]

Nonetheless, the FTC has recently indicated the possibility of formally recommending a self-regulatory system for targeted ads, which is a step in the right direction, but would not provide as much consumer protection as this article advocates.[130] Still, the FTC's roundtable meeting about targeted advertising in November 2007 showed its growing awareness of the privacy issues involved.[131] The recent decision to take action likely reflects that privacy advocates have been pushing online-targeted advertising as the next major privacy-in-cyberspace issue.[132]

127. Yahoo! Privacy, Third Party and Affiliate Cookies on Yahoo!, http://info.yahoo.com/privacy/us/yahoo/ thirdparties/details.html (last visited Apr. 4, 2009).

128. *Id.*

129. *See* discussion *supra* Part I.B.

130. Federal Trade Commission Office of Public Affairs, FTC Staff Proposes Online Behavioral Advertising Privacy Principles (Dec. 20, 2007), http://www.ftc.gov/opa/2007/12/ principles.shtm.

131. Federal Trade Commission Office of Public Affairs, FTC to Host Town Hall to Examine Privacy Issues and Online Behavioral Marketing (Aug. 6. 2007), http://www.ftc.gov/opa/2007/08/ehavioral.shtm.

132. Louise Story, *F.T.C. To Review Online Ads and Privacy*, N.Y. TIMES, Nov. 1, 2007, *available at* http://www.nytimes.com/2007/11/01/technology/ 01Privacy.html?ref=technology.

V. A New Proposed Federal Law Aimed at Online-Targeted Advertising

A. Introduction

Numerous initiatives to address the privacy concerns related to online-targeted advertising, including self-regulation and a "do not track" registry, fail to provide enough protection for consumers.[133] This article proposes federal legislation that would make online-targeted advertising an opt-in program that private companies would administer, but that the FTC would ultimately oversee with the authority to levy hefty fines for non-compliance. Under the legislation, consumers could choose how much personal information to share, but ad companies could never track highly sensitive personal information.

B. Proposal

1. Logistics

The FTC would oversee the practice of targeted advertising, just as the FTC has regulated spyware, under its power to stop unfair and deceptive trade practices. The FTC would conduct random audits of websites to ensure companies kept track of opt-in requests accurately. In addition, the FTC would ensure that the companies kept secure any personal information they collect specifically for targeted marketing, in order to prevent disclosure to unauthorized parties.[134] Finally, the law would authorize the FTC to collect fines from websites that did not comply.

2. Opt-in Program

The most important aspect of the legislation would mandate that all websites and marketers engaged in online-targeted advertising have opt-in policies for all uses of private information that they collect. Implementing the opt-in program would not be through the government, but through the websites and marketing companies themselves.

Under an opt-in program, the consumer could change her mind at any point about whether to be tracked or not. Consumers would be able to

133. Letter from Jeff Chester, Executive Director, Center for Digital Democracy, and Ed Mierzwinski, Consumer Program Director, U.S. PIRG, to Deborah Platt Majoras, Chairman, Federal Trade Commission, Supplemental Statement in Support of Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Online Marketing Practices (Nov. 1, 2007), at 1, *available at* http://www.democraticmedia.org/files/FTCsupplemental_statement 1107.pdf.

134. While the E.C.P.A. requires the safekeeping of personal information, this proposal would include the explicit requirement of securing personal data that companies collect for targeted advertising.

disable programs that track Internet actions. When conducting private Internet surfing, for example, the user could temporarily stop the tracking.

3. Meaningful Notice

The federal bill would require that websites provide meaningful notice about the practice of targeted advertising. Before opting in, the consumers would receive full disclosure, including a complete list of possible uses of the information—such as third-party usage—the reason for collecting the information, and an explanation of the technology tracking the user. The law would require it to use language that the average consumer understood.

The opt-in program with full disclosures would strike the correct balance between speech concerns and property rights because it would allow consumers to receive targeted advertising as long as they had real knowledge about tracking policies.[135] It would also enable consumers to make informed choices about which websites to trust with personal information.

The companies would have to ensure that consent to the collection, use, and exchange of personally identified data is informed and meaningful. Website companies would be able to choose how best to alert people to the notices. They could require users to read the privacy terms before clicking "I agree" or use pop-up boxes to ask permission from the user.

4. No Secondary Use of Information

The law would prohibit unauthorized use of information for a secondary purpose, as opposed to the purpose for which the company collected it. Companies could not sell personal information to another company or use the information for a different purpose besides for the targeted advertisements to which the consumer consented.

Under this proposal, the consumers' rights in the information would follow personal information through "downstream transfers and [limit] the negative effects that result from 'one-shot' permission on all personal data trade."[136]

5. Time Limits

The law would set a time limit of one year during which the company could use information about an individual, then the company would have to

135. Cohen, *supra* note 36, at 1428 (addressing the need for federal legislation on privacy policies to address first amendment speech concerns).

136. Privacy expert Paul Schwartz, who proposes "hybrid inalienability" of personal information, in which individuals can share personal information, discusses this idea and suggests strict limits on the future use of personal information after the initial exchange. Paul M. Schwartz, *Property, Privacy and Personal Data,* 117 HARV. L. REV. 2055, 2094 (2004).

discard it safely.[137] Discarding such information safely could mean destroying it physically or erasing the information from back-up systems.[138]

6. Exceptions

Companies could never use highly sensitive health information for behavioral marketing in order to provide national protection and to ensure that individuals could never make uninformed choices about sharing potentially stigmatizing information. Minimally, companies could not direct ads to people with serious medical conditions, if the companies gleaned such information using online-targeted advertising.

C. Summary

A federal law would provide strong privacy protection to consumers in an area of privacy law that has not yet been tested or challenged. It would require companies using online tracking for targeted marketing to obtain the meaningful consent of the consumers first.

VI. Conclusion

As this article has shown, consumers need federal regulation to address the privacy problems that targeted advertising can cause. The rapidly growing practice has little oversight by the FTC, and no cases have yet tested its boundaries. As such, the practice has the potential to cause increasingly serious privacy harms.

Although the FTC has recently taken an interest in stopping improper online-targeted advertising by hosting roundtable meetings, it has failed to actually pursue marketers engaging in problematic practices or establish regulations. Thus, a federal law specifically aimed at the practice would be the most effective means of regulating abusive practices. The FTC's aggressive campaign against improper spyware shows that spyware poses strikingly similar risks as online-targeted advertising: inadequate consent, buried disclosures, and difficult removal procedures. Such anti-consumer and privacy-eroding practices are also present in much of the targeted advertising industry; therefore federal regulation would ensure the utmost protection of consumer privacy in the future.

137. This rule would exclude aggregated data, which is not linked to individuals, but marketers can utilize it.

138. Long-term collection and storage of data is a problem today, as companies collect more data than they can use with the hopes of finding a use for it sometime in the future. Some companies voluntarily discard personal information right away. Google, for example, searches users' emails to deliver targeted advertising, but it does not store that particular data. Louise Story, *Consumer Advocates Seek a 'Do-Not-Track' List*, N.Y. TIMES (Oct. 31, 2007), *available at* http://www.nytimes.com/ 2007/10/31/technology/31cnd-privacy.html?pagewanted=print.